AMENDMENTS TO THE CLAIMS

1-7 (Canceled)

8. (Previously Presented) A method of monitoring the appropriateness of digital content received at a plurality of monitored computers over a computer network, each of the plurality of monitored computers under the control of a monitored user, the method comprising:

(a) providing a client application comprising data processing executable instructions resident on each of said monitored computers;

(b) providing, in the client application, modules for performing content rating and content filtering;

(c) providing a server application comprising data processing executable instructions resident on a server remotely located from the plurality of monitored computers;

(d) providing at least one communication application in the client application;

(e) providing at least one communication application in the server application;

(f) for the plurality of monitored computers, utilizing said client application to capture in real time all requests for data as the monitored user accesses digital content;

(g) for the plurality of monitored computers, utilizing the at least one communication application of the client application to automatically pass information related to the captured requests for data from the client application to the server in real time as the monitored user accesses the digital content;

(h) for said plurality of monitored computers, utilizing said client application and said server in combination in order to generate an approval or disapproval indication for the digital content in real time as the monitored user accesses the digital content; and

(i) utilizing the client application for blocking or permitting further communication in a predetermined manner in at least partial dependence on the approval or disapproval indication.

9. (Canceled)

10. (Currently Amended) The method of claim 8, further comprising:

sending a signal from the client application to a plurality of servers to determine which server of the plurality of servers has the quickest response rate;

selecting a server with the quickest response rate as a primary server; and

wherein the server on which the server application is resident has been selected as the a primary server.

11. (Previously Presented) The method of claim 8, further comprising:

storing configuration settings on at least one backend server;

wherein the configuration settings relate to user-entered preferences;

sending the configuration settings from the at least one backend server to the client application; and

configuring the client application based in at least partial dependence on the configuration settings.

12. (Previously Presented) The method of claim 8, further comprising:

for the plurality of monitored computers, receiving digital content from the network in response to the requests for data; and

utilizing the client application for delaying delivery of the digital content until the approval or disapproval indication has been generated.

13. (Previously Presented) The method of claim 8, further comprising:

sending updates from the server application to the client application at predetermined intervals; and

configuring the client application based in at least partial dependence on the updates.

14. (Withdrawn) A method of monitoring appropriateness of digital content, the method comprising:

running a client application on an electronic device connected to a network;

wherein the electronic device sends requests for data to the network and digital data is sent from the network to the electronic device in response to the requests;

sending an authentication signal from the client application to a server application resident on at least one server which is remotely disposed from the electronic device;

receiving configuration settings from the server application;

wherein the server application only sends the configuration settings if the authentication signal indicates that a user of the electronic device is a valid user;

configuring the client application based on the configuration settings;

capturing in real time all the requests for data;

sending information based on the requests for data to the server application;

receiving an approval or disapproval indication from the server application in response to the information;

filtering in real time the digital data incoming from the network; and

blocking the digital data if the information is a disapproval indication.

15. (Withdrawn) The method of claim 14, wherein the electronic device comprises at least one of:

a personal computer;

a set-top-box;

a router; and

a gateway.

16. (Withdrawn) The method of claim 14 wherein the client application quarantines the digital data at an application layer at least until the approval or disapproval indication is received.

17. (Withdrawn) The method of claim 14, wherein the configuration settings are based in at least partial dependence on user-entered preferences.

18. (Withdrawn) The method of claim 14, wherein the server application is adapted to provide updated information regarding at least one of emerging threats, content classifications, virus definitions, spyware definitions, phishing threats, Spam sources, and service updates.

19. (Withdrawn) An internet-protection method comprising:

storing account information corresponding to an account in an account database on at least one server interoperably connected to a network;

wherein the account information includes configuration settings for each of at least one valid user;

storing virus definitions in a master virus definitions database on at least one servers;

updating the master virus definitions database at predetermined intervals;

receiving an authentication signal from a client application running on an electronic device interoperably connected to the network;

wherein the authentication signal is used to determine whether the client application corresponds to a valid user account;

transmitting configuration settings to the client application corresponding to the valid user account;

configuring the client application based on the configuration settings transmitted from the one or more servers;

updating a client virus definitions database based on the master virus definitions database;

using the client application to monitor digital data transmitted to the electronic device; and

blocking the digital data if the digital data contains a virus corresponding to a virus definition in the client virus definitions database.

20. (Withdrawn) The internet-protection method of claim 19, wherein the client application is a non-embedded application running on the electronic device.

21. (Withdrawn) The internet-protection method of claim 19, wherein the electronic device comprises at least one of:

a personal computer;

a set-top-box;

a router; and

a gateway.

22. (Withdrawn) The internet-protection method of claim 19, wherein the client application requests updated content rating definitions stored on the server for rating content downloaded from the internet.

23. (Withdrawn) A service-delivery method comprising:

connecting a network interface to an electronic device and a network;

wherein all communication between a client application running on the electronic device and the network passes through the network interface;

sending an authentication signal from the network interface to a backend system interoperably connected to the network interface, the authentication signal providing validation information indicating whether the network interface corresponds to a valid user account;

wherein the backend system comprises configuration settings for configuring the network interface according to the valid user account and updates for updating the network interface;

configuring the network interface according to the configuration settings;

updating the network interface according to the updates;

monitoring all requests for data sent by the client application to the network as the requests pass through the network interface;

monitoring all digital data sent from the network to the client application before the client application receives the digital data;

wherein the network interface delays delivery of the digital data to the electronic device until the digital data has been approved for delivery;

sending a first signal to the backend system based on at least one of the requests for data;

receiving an approval or disapproval indication from the backend system in response to the first signal; and

blocking delivery of digital data sent from the network in response to the at least one of the requests for data responsive to receipt of a disapproval indication from the backend system.

24. (Withdrawn) The service-delivery method of claim 23, further comprising:

sending a second signal to the backend system responsive to digital data sent from the network not being in response to a request for data;

receiving an approval or disapproval indication from the backend system in response to the second signal; and

blocking delivery of digital data sent from the network when a disapproval indication is received from the backend system.

25. (Withdrawn) The service-delivery method of claim 23, wherein the network interface is a router.

26. (Withdrawn) The service-delivery method of claim 23, wherein the backend system is adapted to provide updated information regarding at least one of emerging threats, content classifications, virus definitions, spyware definitions, phishing threats, Spam sources, and service updates.

27. (Withdrawn) The service-delivery method of claim 23, wherein the network interface is adapted to filter the communication between the client application and the network for personal information and requests for inappropriate content.

28. (Withdrawn) The service-delivery method of claim 23, wherein the step of monitoring all requests for data sent by the client application to the network comprises:

copying the requests for data as the requests pass through the network interface;

decoding packet information associated with the requests for data; and

processing the packet information according to the configuration settings.